

Quasi-cyclic Codes of Index $1\frac{1}{2}$

Yun Fan, Hualu Liu

School of Mathematics and Statistics
Central China Normal University, Wuhan 430079, China

Abstract

We introduce quasi-cyclic codes of index $1\frac{1}{2}$, construct such codes in terms of polynomials and matrices; and prove that the quasi-cyclic codes of index $1\frac{1}{2}$ are asymptotically good.

MSC classes: 94B05, 94B65, 15B52.

Key words: Quasi-cyclic code, fractional index, relative minimum distance, random code, asymptotically good code.

1 Introduction

Let F be a finite field. Any subspace C of F^n is called a linear code of length n over F . The fraction $R(C) = \frac{k}{n}$ is called the *rate* of C , where $k = \dim C$ is the dimension of C . The fraction $\Delta(C) = \frac{d}{n}$ is called the *relative minimum distance* of C , where $d = d(C) = \min_{0 \neq \mathbf{c} \in C} w(\mathbf{c})$ is the minimum Hamming distance of C . A sequence C_1, C_2, \dots of codes over F with length n_i of C_i going to infinity is said to be *asymptotically good* if both the rate $R(C_i)$ and the relative minimum distance $\Delta(C_i)$ are positively bounded from below. A class of codes is said to be *asymptotically good* if there exist asymptotically good sequences of codes within the class. By a Varshamov's random argument [14], linear codes are asymptotically good.

Let A be a permutation group on the index set $\{1, 2, \dots, m\}$ of coordinates of F^m . If a linear code C in F^m is invariant by the A -action, i.e. $\alpha(\mathbf{c}) \in C$, $\forall \mathbf{c} \in C \forall \alpha \in A$, then C is said to be an A -acted code ([1]), or an A -permutation code ([6]). If $A = \langle (12 \dots m) \rangle$ is a cyclic group generated by the cycle $(12 \dots m)$ and C is an A -acted code, then C is just the so-called cyclic code of length m . It is a long standing open question (see [10]): *whether or not the cyclic codes are asymptotically good?*

Consider the vector space $F^m \times F^m$ over F with $\{1, 2, \dots, m\}$ and $\{m+1, m+2, \dots, 2m\}$, respectively, being the index sets of coordinates of the first

Email address: yfan@mail.ccnu.edu.cn (Yun Fan). hwlulu@aliyun.com (Hualu Liu).

F^m and the second F^m , respectively. Let $A = \langle (12 \cdots m)(m+1, m+2, \dots, 2m) \rangle$ be the permutation group generated by the product of the corresponding two cycle $(12 \cdots m)$ and $(m+1, m+2, \dots, 2m)$ of length m . Then A is a cyclic group of order m ; and any A -acted code C in $F^m \times F^m$ is said to be a *quasi-cyclic code* of *index 2* and *co-index m* . Similarly, *quasi-cyclic codes* of *index n* and *co-index m* are defined to be the subspaces C of $F^m \times \cdots \times F^m$ (with n copies) which are invariant by the permutation which is the product of n disjoint cycles of length m . Specifically, the quasi-cyclic codes of index 1 and co-index m are just the cyclic codes of length m .

By a random method, [2] showed that, if 2 is primitive for infinitely many primes (this is a so-called *Artin's conjecture*), then asymptotically good binary quasi-cyclic codes of index 2 exist. Later, [3] and [8] made big improvements and proved that, without the Artin's conjecture, the binary quasi-cyclic codes of index 2 are asymptotically good. On the other hand, Ling and Solé [9] showed that self-dual quasi-cyclic codes of co-index 3 and index going to infinity are asymptotically good.

For arbitrary finite group G of order m , any left ideal C of the group ring FG is called a *group code*; and any FG -submodule of $(FG)^n$ is called a *quasi-group code* of *index n* and *co-index m* . If G is abelian, then the quasi-group codes are also called *quasi-abelian codes*, see [4, 15]. Quasi-abelian codes are just quasi-cyclic codes once G is cyclic.

Bazzi and Mitter [1] obtained by a random method two asymptotically good classes of codes: (1) binary quasi-abelian codes of index 2; (2) binary dihedral group codes. Soon after, with the similar random method, Martínez-Pérez and Willems [11] showed that self-dual doubly-even binary dihedral group codes are asymptotically good. By a result [5, Theorem 3.3], the two asymptotically good classes of binary codes obtained in [1] can be extended to any q -ary case. It was also shown in [5] that the quasi-abelian codes with index going to infinity are asymptotically good. The dihedral groups are the non-abelian finite groups which are nearest to cyclic groups. However, if the actions of the involutions (elements of order 2) of the dihedral groups are ignored, then the dihedral group codes can be viewed as quasi-cyclic codes of index 2.

Thus an interesting question we are concerned with comes up: is it possible to consider the quasi-cyclic codes of fractional index between 1 and 2? If it is, are such codes asymptotically good?

In this paper we introduce *quasi-cyclic codes of index $1\frac{1}{2}$* , and show that such codes are asymptotically good.

In Section 2, we define the quasi-cyclic codes of index $1\frac{1}{2}$ and co-index $2m$ to be the subspaces of $F^{2m} \times F^m$ which are invariant by a permutation which is a product of two disjoint cycles of length $2m$ and length m , respectively (hence the permutation generates a cyclic group of order $2m$); and construct such codes in terms of polynomials and matrices.

In section 3, we study a kind of random quasi-cyclic codes of index $1\frac{1}{2}$. We exhibit, in an asymptotic and probabilistic sense, a positive lower bound of

the relative minimal distances of such random codes, see Theorem 3.3 below. Then it follows that asymptotically good quasi-cyclic codes of index $1\frac{1}{2}$ exist, see Theorem 3.5 below.

2 Quasi-cyclic codes of index $1\frac{1}{2}$

From now on, we always assume that F is a finite field with q elements, where q is a power of an odd prime; and m is a positive integer coprime to q . For fundamentals on finite rings and coding theory, please refer to [7, 12].

By $R_{2m} = F[X]/\langle X^{2m} - 1 \rangle$ we denote the residue ring of the polynomial ring $F[X]$ over F modulo the ideal $\langle X^{2m} - 1 \rangle$ generated by $X^{2m} - 1$. Similarly, $R_m = F[X]/\langle X^m - 1 \rangle$. Consider the product

$$R_{2m} \times R_m = F[X]/\langle X^{2m} - 1 \rangle \times F[X]/\langle X^m - 1 \rangle.$$

Each element of $R_{2m} \times R_m$ is uniquely represented as

$$(a(X), a'(X)) \quad \text{with} \quad a(X) = \sum_{j=0}^{2m-1} a_j X^j, \quad a'(X) = \sum_{j'=0}^{m-1} a'_{j'} X^{j'} \in F[X].$$

We always identify the element $(a(X), a'(X)) \in R_{2m} \times R_m$ with the word

$$(a_0, a_1, \dots, a_{2m-2}, a_{2m-1}, a'_0, a'_1, \dots, a'_{m-2}, a'_{m-1}) \in F^{2m} \times F^m.$$

Let ξ be a permutation of the coefficients of $F^{2m} \times F^m$, which is a product of two disjoint cycles of length $2m$ and m , respectively, as follows:

$$\begin{aligned} & \xi(a_0, a_1, \dots, a_{2m-2}, a_{2m-1}, a'_0, a'_1, \dots, a'_{m-2}, a'_{m-1}) \\ &= (a_{2m-1}, a_0, a_1, \dots, a_{2m-2}, a'_{m-1}, a'_0, a'_1, \dots, a'_{m-2}). \end{aligned}$$

The permutation ξ on $F^{2m} \times F^m$ is corresponding to the operation on $R_{2m} \times R_m$ by multiplying X : for $a(X) = \sum_{j=0}^{2m-1} a_j X^j$ and $a'(X) = \sum_{j'=0}^{m-1} a'_{j'} X^{j'}$,

$$X(a(X), a'(X)) = (Xa(X) \pmod{X^{2m} - 1}, Xa'(X) \pmod{X^m - 1}). \quad (2.1)$$

Definition 2.1. A linear subspace C of $R_{2m} \times R_m$ is said to be a *quasi-cyclic code over F of index $1\frac{1}{2}$ and co-index $2m$* if C is invariant by the permutation ξ , i.e.

$$X(c(X), c'(X)) \in C, \quad \forall (c(X), c'(X)) \in C.$$

The operation (2.1) can be extended in a natural way: for any $f(X) \in F[X]$ and any $(a(X), a'(X)) \in R_{2m} \times R_m$,

$$\begin{aligned} & f(X)(a(X), a'(X)) \\ &= (f(X)a(X) \pmod{X^{2m} - 1}, f(X)a'(X) \pmod{X^m - 1}). \end{aligned} \quad (2.1')$$

To shorten the notation, in the following we abbreviate the operation (2.1') on $R_{2m} \times R_m$ as:

$$f(X)(a(X), a'(X)) = (f(X)a(X), f(X)a'(X)).$$

Obviously, a linear subspace C of $R_{2m} \times R_m$ is a quasi-cyclic code of index $1\frac{1}{2}$ and co-index $2m$ if and only if it is invariant by multiplying any $f(X) \in F[X]$. In other words, $R_{2m} \times R_m$ is an $F[X]$ -module (or, R_{2m} -module), and its $F[X]$ -submodules (R_{2m} -modules) are just the quasi-cyclic codes of index $1\frac{1}{2}$ and co-index $2m$.

An $F[X]$ -submodule of $R_{2m} \times R_m$ is generated by at most two elements. For our later use, we illustrate a kind of quasi-cyclic codes of index $1\frac{1}{2}$ and co-index $2m$, each of which is generated by one element.

Example 2.2. For $(a(X), a'(X)) \in R_{2m} \times R_m$, let

$$C_{a,a'} = \{ (f(X)a(X), f(X)a'(X)) \in R_{2m} \times R_m \mid f(X) \in R_{2m} \}. \quad (2.2)$$

Then $C_{a,a'}$ is a quasi-cyclic code of index $1\frac{1}{2}$ and co-index $2m$. Further, let

$$\begin{aligned} a(X) &= a_0 + a_1X + \cdots + a_{2m-1}X^{2m-1}, \\ a'(X) &= a'_0 + a'_1X + \cdots + a'_{m-1}X^{m-1}. \end{aligned}$$

For $a(X)$ we have a $2m$ -dimensional vector $(a_0, a_1, \dots, a_{2m-2}, a_{2m-1})$, from which a circulant $2m \times 2m$ matrix is constructed as follows:

$$A = \begin{pmatrix} a_0 & a_1 & \cdots & a_{2m-2} & a_{2m-1} \\ a_{2m-1} & a_0 & \cdots & a_{2m-3} & a_{2m-2} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_2 & a_3 & \cdots & a_0 & a_1 \\ a_1 & a_2 & \cdots & a_{2m-1} & a_0 \end{pmatrix}_{2m \times 2m}.$$

Similarly, from $a'(X)$ we have a circulant $m \times m$ matrix as follows:

$$A' = \begin{pmatrix} a'_0 & a'_1 & \cdots & a'_{m-2} & a'_{m-1} \\ a'_{m-1} & a'_0 & \cdots & a'_{m-3} & a'_{m-2} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a'_2 & a'_3 & \cdots & a'_0 & a'_1 \\ a'_1 & a'_2 & \cdots & a'_{m-1} & a'_0 \end{pmatrix}_{m \times m}.$$

Then we can construct a $2m \times 3m$ matrix:

$$\hat{A} = \begin{pmatrix} A & A' \\ A' & A' \end{pmatrix}_{2m \times 3m}. \quad (2.3)$$

And it is easy to see that

$$C_{a,a'} = \{ (y_0, y_1, \dots, y_{2m-1})\hat{A} \in F^{2m} \times F^m \mid (y_0, y_1, \dots, y_{2m-1}) \in F^{2m} \}.$$

Note that \hat{A} is not a generator matrix of the code $C_{a,a'}$ in general, since it is not of rank $2m$ in general. After Theorem 2.4 below, we'll see how to get a generator matrix of $C_{a,a'}$ from the matrix \hat{A} .

Remark 2.3. For $X^{2m} - 1$, we have the following facts:

$$X^{2m} - 1 = (X^m + 1)(X^m - 1), \quad \frac{1}{2}(X^m + 1) + \frac{-1}{2}(X^m - 1) = 1.$$

By Chinese Remainder Theorem, we have the natural isomorphism:

$$\begin{aligned} \frac{F[X]}{\langle X^{2m}-1 \rangle} &\xrightarrow{\cong} \frac{F[X]}{\langle X^m-1 \rangle} \times \frac{F[X]}{\langle X^m+1 \rangle}, \\ f(X) &\mapsto (f(X) \pmod{X^m-1}, f(X) \pmod{X^m+1}). \end{aligned} \quad (2.4)$$

In the following, for any polynomial $f(X)$, by $\langle f(X) \rangle_{R_{2m}}$ we clarify that it is an ideal of R_{2m} generated by $f(X)$. It is easy to check that the isomorphism (2.4) induces a direct sum:

$$R_{2m} = \langle X^m + 1 \rangle_{R_{2m}} \oplus \langle X^m - 1 \rangle_{R_{2m}},$$

and two natural isomorphisms:

$$\begin{aligned} \langle X^m + 1 \rangle_{R_{2m}} &\xrightarrow{\cong} F[X]/\langle X^m - 1 \rangle, \\ \langle X^m - 1 \rangle_{R_{2m}} &\xrightarrow{\cong} F[X]/\langle X^m + 1 \rangle. \end{aligned} \quad (2.5)$$

Theorem 2.4. Given any $(a(X), a'(X)) \in R_{2m} \times R_m$. Let

$$g_{a,a'}(X) = \gcd(a(X), X^m + 1) \cdot \gcd(a(X), a'(X), X^m - 1) \quad (2.6)$$

where $\gcd(\dots)$ denotes the greatest common divisor, and let

$$h_{a,a'}(X) = \frac{X^{2m} - 1}{g_{a,a'}(X)}.$$

Then $(a(X), a'(X))$ induces an $F[X]$ -homomorphism

$$\gamma_{a,a'} : R_{2m} \longrightarrow R_{2m} \times R_m, \quad f(X) \mapsto (f(X)a(X), f(X)a'(X)),$$

and the following hold:

- (i) The image $\text{im}(\gamma_{a,a'}) = C_{a,a'}$, where $C_{a,a'}$ is defined in Eqn (2.2).
- (ii) The kernel $\ker(\gamma_{a,a'}) = \langle h_{a,a'}(X) \rangle_{R_{2m}}$, hence $\dim C_{a,a'} = \deg h_{a,a'}(X)$.
- (iii) $\gamma_{a,a'}$ induces an isomorphism $\langle g_{a,a'}(X) \rangle_{R_{2m}} \xrightarrow{\cong} C_{a,a'}$; in particular,

$$C_{a,a'} = \{ (b(X)a(X), b(X)a'(X)) \in R_{2m} \times R_m \mid b(X) \in \langle g_{a,a'}(X) \rangle_{R_{2m}} \}.$$

Proof. It is obvious that $\gamma_{a,a'}$ is an $F[X]$ -homomorphism and (i) holds.

For (ii), $f(X) \in \ker(\gamma_{a,a'})$ if and only if

$$\begin{cases} f(X)a(X) \equiv 0 \pmod{X^{2m}-1}, \\ f(X)a'(X) \equiv 0 \pmod{X^m-1}. \end{cases} \quad (2.7)$$

By the isomorphism (2.4), the system (2.7) is equivalent to the following system:

$$\begin{cases} f(X)a(X) \equiv 0 & (\text{mod } X^m + 1), \\ f(X)a(X) \equiv 0 & (\text{mod } X^m - 1), \\ f(X)a'(X) \equiv 0 & (\text{mod } X^m - 1). \end{cases}$$

The last two equations are combined into one equation:

$$f(X) \gcd(a(X), a'(X)) \equiv 0 \pmod{X^m - 1}.$$

So the system (2.7) is equivalent to:

$$\begin{cases} f(X) \equiv 0 & (\text{mod } \frac{X^m + 1}{\gcd(a(X), X^m + 1)}), \\ f(X) \equiv 0 & (\text{mod } \frac{X^m - 1}{\gcd(a(X), a'(X), X^m - 1)}). \end{cases}$$

Since $\frac{X^m + 1}{\gcd(a(X), X^m + 1)}$ and $\frac{X^m - 1}{\gcd(a(X), a'(X), X^m - 1)}$ are coprime to each other, we see that the system (2.7) holds if and only if

$$f(X) \equiv 0 \pmod{\frac{X^m + 1}{\gcd(a(X), X^m + 1)} \cdot \frac{X^m - 1}{\gcd(a(X), a'(X), X^m - 1)}},$$

that is, $f(X) \in \langle h_{a,a'}(X) \rangle_{R_{2m}}$. In particular,

$$\dim C_{a,a'} = \dim R_{2m} - \dim \ker(\gamma_{a,a'}) = 2m - \deg g_{a,a'}(X) = \deg h_{a,a'}(X).$$

We are done for (ii).

Finally, since $X^{2m} - 1$ has no multiple roots (i.e., R_{2m} is semisimple),

$$R_{2m} = \langle h_{a,a'}(X) \rangle_{R_{2m}} \oplus \langle g_{a,a'}(X) \rangle_{R_{2m}}.$$

And the kernel of the homomorphism $\gamma_{a,a'}$ is just the ideal $\langle h_{a,a'}(X) \rangle_{R_{2m}}$. So, (iii) is proved. \square

Example 2.5. Take $q = 3$, $m = 2$, $a(X) = (X - 1)(X^2 + 1) = X^3 + 2X^2 + X + 2$ and $a'(X) = X + 1$. By Theorem 2.4,

$$g_{a,a'}(X) = \gcd(a(X), X^2 + 1) \gcd(a(X), a'(X), X^2 - 1) = X^2 + 1;$$

$$h_{a,a'}(X) = (X^4 - 1)/g_{a,a'}(X) = X^2 - 1.$$

So $\dim C_{a,a'} = 2$. Using the notations in Example 2.2, we have

$$A = \begin{pmatrix} 2 & 1 & 2 & 1 \\ 1 & 2 & 1 & 2 \\ 2 & 1 & 2 & 1 \\ 1 & 2 & 1 & 2 \end{pmatrix}, \quad A' = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix};$$

$$\hat{A} = \begin{pmatrix} 2 & 1 & 2 & 1 & 1 & 1 \\ 1 & 2 & 1 & 2 & 1 & 1 \\ 2 & 1 & 2 & 1 & 1 & 1 \\ 1 & 2 & 1 & 2 & 1 & 1 \end{pmatrix}.$$

Thus the first two rows of \widehat{A} are linearly independent and

$$G = \begin{pmatrix} 2 & 1 & 2 & 1 & 1 & 1 \\ 1 & 2 & 1 & 2 & 1 & 1 \end{pmatrix}$$

is a generator matrix of $C_{a,a'}$. The 9 codewords of $C_{a,a'}$ are as follows:

$$\begin{array}{cccccc} 000000 & 212111 & 121222 & 121211 & 212122 \\ 000022 & 000011 & 121200 & 212100 \end{array}$$

Example 2.6. Take $q = 3$, $m = 2$, $a(X) = X - 1 = X + 2$ and $a'(X) = X - 1$. By Theorem 2.4,

$$\begin{aligned} g_{a,a'}(X) &= \gcd(a(X), X^2 + 1) \gcd(a(X), a'(X), X^2 - 1) = X - 1; \\ h_{a,a'}(X) &= (X^4 - 1)/g_{a,a'}(X) = (X^2 + 1)(X + 1). \end{aligned}$$

So $\dim C_{a,a'} = 3$. And by the notations in Example 2.2,

$$A = \begin{pmatrix} 2 & 1 & & & & \\ & 2 & 1 & & & \\ & & 2 & 1 & & \\ 1 & & & & 2 & \end{pmatrix}, \quad A' = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix};$$

$$\widehat{A} = \begin{pmatrix} 2 & 1 & & & 2 & 1 \\ & 2 & 1 & & 1 & 2 \\ & & 2 & 1 & 2 & 1 \\ 1 & & & 2 & 1 & 2 \end{pmatrix}.$$

Thus the first three rows of \widehat{A} are linearly independent and

$$G = \begin{pmatrix} 2 & 1 & & & 2 & 1 \\ & 2 & 1 & & 1 & 2 \\ & & 2 & 1 & 2 & 1 \end{pmatrix}$$

is a generator matrix of $C_{a,a'}$. The 27 codewords of $C_{a,a'}$ are as follows.

$$\begin{array}{ccccccc} 000000 & 002121 & 001212 & 021012 & 020100 & 022221 & 012021 \\ 011112 & 010200 & 210021 & 212112 & 211200 & 201000 & 200121 \\ 202212 & 222012 & 221100 & 220221 & 120012 & 122100 & 121221 \\ 111021 & 110112 & 112200 & 102000 & 101121 & 100212 \end{array}$$

From Example 2.2, we construct a class of quasi-cyclic codes of index $1\frac{1}{2}$ and co-index $2m$, which will be used in the next section.

Example 2.7. Consider an ideal J_{2m}^+ of R_{2m} and an ideal J_m of R_m as follows:

$$J_{2m}^+ = \langle (X^m + 1)(X - 1) \rangle_{R_{2m}}, \quad J_m = \langle X - 1 \rangle_{R_m}. \quad (2.8)$$

For any $a(X) \in J_{2m}^+$ and $a'(X) \in J_m$, as illustrated in Example 2.2, the code $C_{a,a'} = \{(f(X)a(X), f(X)a'(X)) \in R_{2m} \times R_m \mid f(X) \in R_{2m}\}$ is a quasi-cyclic code of index $1\frac{1}{2}$ and co-index $2m$. By the definition of J_{2m}^+ and J_m in Eqn (2.8),

$$\gcd(a(X), X^m + 1) = X^m + 1, \quad (X - 1) \mid \gcd(a(X), a'(X), X^m - 1).$$

So $(X^m + 1)(X - 1) \mid g_{a,a'}(X)$, where $g_{a,a'}(X)$ is defined in Eqn (2.6). Then

$$\langle g_{a,a'}(X) \rangle_{R_{2m}} \subseteq \langle (X^m + 1)(X - 1) \rangle_{R_{2m}} = J_{2m}^+.$$

By Theorem 2.4 (iii), instead of R_{2m} , the quasi-cyclic code $C_{a,a'}$ of index $1\frac{1}{2}$ and co-index $2m$ can be formed within J_{2m}^+ as follows:

$$C_{a,a'} = \{(b(X)a(X), b(X)a'(X)) \in R_{2m} \times R_m \mid b(X) \in J_{2m}^+\}. \quad (2.9)$$

Remark 2.8. Let $\frac{X^m-1}{X-1} = p_1(X) \cdots p_h(X)$ be an irreducible decomposition of $\frac{X^m-1}{X-1}$ in $F[X]$, i.e., all the $p_j(X)$'s are irreducible polynomials over F . For $j = 1, \dots, h$, by Eqn (2.5), the following is a surjective homomorphism:

$$\mu_{2m}^{(j)} : J_{2m}^+ \rightarrow F[X]/\langle p_j(X) \rangle, \quad a(X) \mapsto a(X) \pmod{p_j(X)}.$$

And, by Chinese Remainder Theorem, we have an isomorphisms as follows.

$$\begin{aligned} \mu_{2m} : J_{2m}^+ &\rightarrow F[X]/\langle p_1(X) \rangle \times \cdots \times F[X]/\langle p_h(X) \rangle, \\ a(X) &\mapsto \left(\mu_{2m}^{(1)}(a(X)), \dots, \mu_{2m}^{(h)}(a(X)) \right). \end{aligned} \quad (2.10)$$

Similarly, for J_m we have surjective homomorphisms as follows.

$$\mu_m^{(j)} : J_m \rightarrow F[X]/\langle p_j(X) \rangle, \quad a'(X) \mapsto a'(X) \pmod{p_j(X)}; \quad j = 1, \dots, h.$$

And an isomorphisms is as follows.

$$\begin{aligned} \mu_m : J_m &\rightarrow F[X]/\langle p_1(X) \rangle \times \cdots \times F[X]/\langle p_h(X) \rangle, \\ a'(X) &\mapsto \left(\mu_m^{(1)}(a'(X)), \dots, \mu_m^{(h)}(a'(X)) \right). \end{aligned}$$

In particular, $\dim J_{2m}^+ = \dim J_m = m - 1$.

Lemma 2.9. *Let notations be as in Remark 2.8, let $(a(X), a'(X)) \in J_{2m}^+ \times J_m$. Then $\dim C_{a,a'} \leq m - 1$; and $\dim C_{a,a'} < m - 1$ if and only if there is an index j with $1 \leq j \leq h$ such that $\mu_{2m}^{(j)}(a(X)) = 0 = \mu_m^{(j)}(a'(X))$.*

Proof. From the assumption of the lemma and the isomorphisms μ_{2m} and μ_m in Remark 2.8, it is easy to see that $\gcd(a(X), X^m + 1) = X^m + 1$ and

$$\gcd(a(X), a'(X), X^m - 1) = (X - 1) \prod_{\mu_{2m}^{(j)}(a(X))=0=\mu_m^{(j)}(a'(X))} p_j(X).$$

The conclusions follow from Theorem 2.4. \square

Lemma 2.10. *Let notations be as in Remark 2.8, let*

$$\ell_m = \min\{\deg p_1(X), \dots, \deg p_h(X)\}. \quad (2.11)$$

Then any non-zero ideal of R_{2m} which are contained in J_{2m}^+ has dimension at least ℓ_m , and the number of the ideals of dimension d (with $\ell_m \leq d < m$) which are contained in J_{2m}^+ is at most $m^{\frac{d}{\ell_m}}$.

Proof. By the isomorphism (2.10), each irreducible ideal contained in J_{2m}^+ is corresponding to exact one irreducible divisor of $\frac{X^m-1}{X-1}$ such that the dimension of the ideal is equal to the degree of the corresponding divisor. Thus, the minimal dimension of the ideals contained in J_{2m}^+ is equal to ℓ_m . And, any d -dimensional ideal contained in J_{2m}^+ is a sum of at most d/ℓ_m irreducible ideals. So the number of the d -dimensional ideals contained in J_{2m}^+ is at most the partial sum of binomial coefficients $\sum_{i=1}^{\lfloor d/\ell_m \rfloor} \binom{h}{i}$, where h is the number of the irreducible ideals contained in J_{2m}^+ (as in Remark 2.8) and $\lfloor d/\ell_m \rfloor$ denotes the largest integer which is not larger than d/ℓ_m . It is easy to check that the partial sum is not larger than m^{d/ℓ_m} . \square

3 Random quasi-cyclic codes of index $1\frac{1}{2}$

Keep the notations in Section 2.

Let $h_q(x) = x \log_q(q-1) - x \log_q x - (1-x) \log_q(1-x)$ with the convention that $0 \log_q 0 = 0$, it is called the q -ary entropy. Note that $h_q(x)$ is a strictly increasing concave function in the interval $[0, 1 - q^{-1}]$ with $h_q(0) = 0$ and $h_q(1 - q^{-1}) = 1$, see [7, §2.10.6]. Hence, in the interval $[0, 1]$, the inverse function $h_q^{-1}(x)$ exists and it is a strictly increasing convex function with $h_q^{-1}(0) = 0$ and $h_q^{-1}(1) = 1 - q^{-1}$. Specifically, $h_q^{-1}(1/2) < 1/2$.

In the following, we always assume that δ is a positive real number less than $\frac{2}{3}h_q^{-1}(\frac{1}{2})$; i.e.,

$$0 < \delta < \frac{2}{3}h_q^{-1}(\frac{1}{2}) < \frac{1}{3}. \quad (3.1)$$

Let $J_{2m}^+ = \langle (X^m + 1)(X - 1) \rangle_{R_{2m}}$ and $J_m = \langle X - 1 \rangle_{R_m}$ as in Eqn (2.8) of Example 2.7. In this section we view the set $J_{2m}^+ \times J_m$ as a probability space, whose samples are afforded with equal probability. We will study a kind of random quasi-cyclic codes of index $1\frac{1}{2}$ over the probability space. As a preparation, we introduce a type of 0-1 variables.

Given any $b(X) \in J_{2m}^+$. We define a Bernoulli variable X_b over the probability space $J_{2m}^+ \times J_m$ as follows: for all samples $(a(X), a'(X)) \in J_{2m}^+ \times J_m$,

$$X_b = \begin{cases} 1, & 1 \leq w(b(X)a(X), b(X)a'(X)) \leq 3m\delta; \\ 0, & \text{otherwise.} \end{cases} \quad (3.2)$$

Since $b(X) \in J_{2m}^+$, the set $\{b(X)a(X) \in R_{2m} \mid a(X) \in J_{2m}^+\}$ is the ideal of R_{2m} generated by $b(X)$, we denote it by I_b and denote its dimension by d_b ; i.e.,

$$I_b = \langle b(X) \rangle_{R_{2m}} \subseteq J_{2m}^+, \quad d_b = \dim I_b. \quad (3.3)$$

In R_m , since $b(X) \in J_m$, we get an ideal

$$I'_b = \langle b(X) \rangle_{R_m} = \{b(X)a'(X) \in R_m \mid a'(X) \in J_m\} \subseteq J_m.$$

Note that $\dim I'_b = \dim I_b = d_b$ (cf. Remark 2.8). We show an estimation of the expectation $E(X_b)$ of the random variable X_b for later quotation.

Lemma 3.1. *Let notations be as in Eqns (3.1)-(3.3). Then*

$$E(X_b) \leq q^{-2d_b + 2d_b h_q(\frac{3}{2}\delta) + \log_q m}.$$

Proof. Given any $b(X) \in J_{2m}^+$. We have an R_{2m} -homomorphism

$$\begin{aligned} \rho_b : \quad J_{2m}^+ \times J_m &\longrightarrow J_{2m}^+ \times J_m, \\ (a(X), a'(X)) &\longmapsto (b(X)a(X), b(X)a'(X)). \end{aligned}$$

Then the image of ρ_b is

$$\text{im}(\rho_b) = I_b \times I'_b = \langle b(X) \rangle_{R_{2m}} \times \langle b(X) \rangle_{R_m}.$$

Let $(I_b \times I'_b)^{\leq \delta}$ denote the set of the words in $I_b \times I'_b$ whose *relative weights* (the ratio of the Hamming weight to the length) are at most δ , i.e.,

$$(I_b \times I'_b)^{\leq \delta} = \{(c(X), c'(X)) \in I_b \times I'_b \mid \frac{w(c(X), c'(X))}{3m} \leq \delta\}.$$

Since X_b is a 0-1-variable, the expectation of X_b is just the probability that $X_b = 1$, that is,

$$E(X_b) = \Pr(X_b = 1) = \frac{|(I_b \times I'_b)^{\leq \delta}| - 1}{|I_b \times I'_b|},$$

where $|S|$ denotes the cardinality of any set S . It is clear that

$$(I_b \times I'_b)^{\leq \delta} \subseteq \bigcup_{w_1, w_2 \geq 0, w_1 + w_2 = \lfloor 3m\delta \rfloor} I_b^{\leq \frac{w_1}{2m}} \times I'_b^{\leq \frac{w_2}{m}},$$

where $\lfloor 3m\delta \rfloor$ denotes the largest integer which is not larger than $3m\delta$. Note that R_{2m} (R_m respectively) is a group ring of a cyclic group of order $2m$ (order m respectively), and I_b (I'_b respectively) is an ideal of R_{2m} (R_m respectively). By [5, Theorem 3.3] and [5, Remark 3.2] we obtain that

$$|I_b^{\leq \frac{w_1}{2m}}| \leq q^{d_b h_q(\frac{w_1}{2m})}, \quad |I'_b^{\leq \frac{w_2}{m}}| \leq q^{d_b h_q(\frac{w_2}{m})}.$$

So

$$\begin{aligned}
|(I_b \times \bar{I}_b)^{\leq \delta}| &\leq \sum_{w_1, w_2 \geq 0, w_1 + w_2 = \lfloor 3m\delta \rfloor} q^{d_b h_q(\frac{w_1}{2m})} \cdot q^{d_b h_q(\frac{w_2}{m})} \\
&= \sum_{w_1, w_2 \geq 0, w_1 + w_2 = \lfloor 3m\delta \rfloor} q^{d_b \left(h_q(\frac{w_1}{2m}) + h_q(\frac{w_2}{m}) \right)}.
\end{aligned}$$

Since $h_q(x)$ is a concave function in $[0, 1]$ and both $\frac{w_1}{2m}, \frac{w_2}{m} \in [0, 1]$ (recall that $\delta < \frac{1}{3}$), we have

$$h_q\left(\frac{w_1}{2m}\right) + h_q\left(\frac{w_2}{m}\right) \leq 2h_q\left(\frac{\frac{w_1}{2m} + \frac{w_2}{m}}{2}\right) = 2h_q\left(\frac{w_1 + 2w_2}{4m}\right).$$

Note that $w_1 + w_2 = \lfloor 3m\delta \rfloor$ and $\delta < \frac{1}{3}$. We see that

$$\frac{w_1 + 2w_2}{4m} \leq \frac{2w_1 + 2w_2}{4m} = \frac{3}{2}\delta < \frac{1}{2} \leq 1 - q^{-1}.$$

And $h_q(x)$ is increasing in the interval $(0, 1 - q^{-1})$, so

$$|(I_b \times I'_b)^{\leq \delta}| \leq 3m\delta \cdot q^{2d_b h_q(\frac{3\delta}{2})} \leq q^{2d_b h_q(\frac{3\delta}{2}) + \log_q m}.$$

Thus

$$E(X_b) \leq \frac{|(I_b \times I'_b)^{\leq \delta}|}{|I_b \times I'_b|} \leq q^{-2d_b + 2d_b h_q(\frac{3\delta}{2}) + \log_q m}. \quad \square$$

From Eqn (2.9) of Example 2.7, we have the quasi-cyclic code of index $1\frac{1}{2}$ and co-index $2m$:

$$C_{a,a'} = \{(b(X)a(X), b(X)a'(X)) \in R_{2m} \times R_m \mid b(X) \in J_{2m}^+\}, \quad (3.4)$$

where $(a(X), a'(X)) \in J_{2m}^+ \times J_m$. Since $J_{2m}^+ \times J_m$ is a probability space, $C_{a,a'}$ is a random code over this probability space, hence the relative distance $\Delta(C_{a,a'})$ of $C_{a,a'}$ is a random variable over the probability space. We present an estimation of the probability that $\Delta(C_{a,a'})$ is at most δ .

Lemma 3.2. *Let δ be as in Eqn (3.1) and $C_{a,a'}$ be as in Eqn (3.4). Let ℓ_m be the minimal degree of the irreducible divisors of $\frac{X^m - 1}{X - 1}$ as in Eqn (2.11). Then*

$$\Pr(\Delta(C_{a,a'}) \leq \delta) \leq \sum_{j=\ell_m}^{m-1} q^{-2j \left(\frac{1}{2} - h_q(\frac{3\delta}{2}) - \frac{\log_q m}{\ell_m} \right)}.$$

Proof. Let X_b for $b(X) \in J_{2m}^+$ be the 0-1-variable in Eqn (3.2). Let

$$X = \sum_{b(X) \in J_{2m}^+} X_b.$$

Then X is a non-negative integer random variable over the probability space $J_{2m}^+ \times J_m$. By Eqn (3.2) and Eqn (3.4), X stands for the number of $b(X) \in J_{2m}^+$ such that the codeword $(b(X)a(X), b(X)a'(X))$ is non-zero and has Hamming weight at most $3m\delta$. Thus

$$\Pr(\Delta(C_{a,a'}) \leq \delta) = \Pr(X > 0).$$

By a Markov's inequality [13, Theorem 3.1], $\Pr(X > 0) \leq E(X)$. So we can prove the lemma by estimating the expectation $E(X)$.

By the linearity of the expectation, $E(X) = \sum_{b(X) \in J_{2m}^+} E(X_b)$. For any ideal I of J_{2m}^+ (we denote it by $I \leq J_{2m}^+$), let $I^* = \{b(X) \in I \mid I_b = I\}$, where I_b is defined in Eqn (3.3). That is,

$$I^* = \{b(X) \in I \mid d_b = \dim I\},$$

where $d_b = \dim I_b$, see Eqn (3.3). It is easy to see that $J_{2m}^+ = \bigcup_{I \leq J_{2m}^+} I^*$, where the subscript " $I \leq J_{2m}^+$ " means that I runs over the ideals contained in J_{2m}^+ . By Lemma 2.10, if $0 \neq I \leq J_{2m}^+$ then $\ell_m \leq \dim I \leq m-1$. So

$$E(X) = \sum_{I \leq J_{2m}^+} \sum_{b(X) \in I^*} E(X_b) = \sum_{j=\ell_m}^{m-1} \sum_{\substack{I \leq J_{2m}^+ \\ \dim I = j}} \sum_{b(X) \in I^*} E(X_b).$$

For $I \leq J_{2m}^+$ with $\dim I = j$, by Lemma 3.1 and the fact that $|I^*| \leq |I| = q^j$, we get

$$\sum_{b(X) \in I^*} E(X_b) \leq \sum_{b(X) \in I^*} q^{-2j+2jh_q(\frac{3}{2}\delta)+\log_q m} \leq q^{-j+2jh_q(\frac{3}{2}\delta)+\log_q m}.$$

By Lemma 2.10 again, the number of $I \leq J_{2m}^+$ with $\dim I = j$ is less than m^{j/ℓ_m} . And note that $\log_q m \leq \frac{j \log_q m}{\ell_m}$ (as $j \geq \ell_m$). So

$$\begin{aligned} E(X) &\leq \sum_{j=\ell_m}^{m-1} m^{j/\ell_m} q^{-j+2jh_q(\frac{3}{2}\delta)+\log_q m} \\ &\leq \sum_{j=\ell_m}^{m-1} q^{-2j(\frac{1}{2}-h_q(\frac{3}{2}\delta)-\frac{\log_q m}{\ell_m})}. \end{aligned}$$

The lemma is proved. \square

By [1, Lemma 2.6], there are positive integers m_1, m_2, \dots satisfying that

$$\gcd(m_i, q) = 1, \quad m_i \rightarrow \infty, \quad \lim_{i \rightarrow \infty} \frac{\log_q m_i}{\ell_{m_i}} = 0, \quad (3.5)$$

where ℓ_{m_i} is the minimal degree of the irreducible divisors of $\frac{X^{m_i}-1}{X-1}$ as defined in Eqn (2.11).

Theorem 3.3. Let m_1, m_2, \dots be positive integers satisfying Eqn (3.5). For each m_i , let $C_{a,a'}^{(i)}$ be the random quasi-cyclic code of index $1\frac{1}{2}$ and co-index $2m_i$ as in Eqn (3.4). If $0 < \delta < \frac{2}{3}h_q^{-1}(\frac{1}{2})$, then

$$\lim_{i \rightarrow \infty} \Pr(\Delta(C_{a,a'}^{(i)}) > \delta) = 1.$$

Proof. Because of the assumption on δ , we have $\frac{1}{2} - h_q(\frac{3}{2}\delta) > 0$. By Eqn (3.5), there are a positive real number β and an integer N such that

$$\frac{1}{2} - h_q(\frac{3}{2}\delta) - \frac{\log_q m_i}{\ell_{m_i}} \geq \beta, \quad \forall i > N.$$

By Lemma 3.2,

$$\begin{aligned} \lim_{i \rightarrow \infty} \Pr(\Delta(C_{a,a'}^{(i)}) \leq \delta) &\leq \lim_{i \rightarrow \infty} \sum_{j=\ell_{m_i}}^{m_i-1} q^{-2j\beta} \leq \lim_{i \rightarrow \infty} \sum_{j=\ell_{m_i}}^{m_i-1} q^{-2\ell_{m_i}\beta} \\ &\leq \lim_{i \rightarrow \infty} m_i q^{-2\ell_{m_i}\beta} = \lim_{i \rightarrow \infty} q^{-2\ell_{m_i}(\beta - \frac{\log_q m_i}{2\ell_{m_i}})}. \end{aligned}$$

Since $\lim_{i \rightarrow \infty} \frac{\log_q m_i}{2\ell_{m_i}} = 0$ (which implies that $\lim_{i \rightarrow \infty} \ell_{m_i} = \infty$), we obtain that

$$\lim_{i \rightarrow \infty} \Pr(\Delta(C_{a,a'}^{(i)}) \leq \delta) = 0. \quad \square$$

Next, we estimate the rate $R(C_{a,a'}^{(i)})$ of the random code $C_{a,a'}^{(i)}$.

Theorem 3.4. Let m_1, m_2, \dots be positive integers satisfying Eqn (3.5). For each m_i , let $C_{a,a'}^{(i)}$ be the random quasi-cyclic code of index $1\frac{1}{2}$ and co-index $2m_i$ as in Eqn (3.4). Then

$$\lim_{i \rightarrow \infty} \Pr(\dim C_{a,a'}^{(i)} = m_i - 1) = 1.$$

Proof. Let $\frac{X^{m_i}-1}{X-1} = p_1(X) \cdots p_{h_i}(X)$ be the irreducible decomposition in $F[X]$ as in Remark 2.8. By Lemma 2.9 and its notations, $\dim C_{a,a'}^{(i)} = m_i - 1$ if and only if for any $j = 1, \dots, h_i$, in $F[X]/\langle p_j(X) \rangle \times F[X]/\langle p_j(X) \rangle$ the following holds:

$$(\mu_{2m_i}^{(j)}(a(X)), \mu_{m_i}^{(j)}(a'(X))) \neq (0, 0), \quad (3.6)$$

where $\mu_{2m_i}^{(j)} : J_{2m_i}^+ \rightarrow F[X]/\langle p_j(X) \rangle$ and $\mu_{m_i}^{(j)} : J_{m_i} \rightarrow F[X]/\langle p_j(X) \rangle$ are surjective homomorphisms defined in Remark 2.8.

Let $d_j = \deg p_j(X)$. Then $F[X]/\langle p_j(X) \rangle$ is a finite field of cardinality q^{d_j} . So the probability that Eqn (3.6) holds is equal to $\frac{q^{2d_j}-1}{q^{2d_j}} = 1 - q^{-2d_j}$. Obviously, the events that Eqn (3.6) holds for $j = 1, \dots, h_i$ are randomly independent. Thus

$$\Pr(\dim C_{a,a'}^{(i)} = m_i - 1) = \prod_{j=1}^{h_i} (1 - q^{-2d_j}).$$

By definition of ℓ_{m_i} in Eqn (2.11), $\ell_{m_i} \leq d_j$ for $j = 1, \dots, h_i$; hence $h_i \leq \frac{m_i-1}{\ell_{m_i}} \leq \frac{m_i}{\ell_{m_i}}$. Thus

$$\begin{aligned} \Pr(\dim C_{a,a'}^{(i)} = m_i - 1) &\geq (1 - q^{-2\ell_{m_i}})^{\frac{m_i}{\ell_{m_i}}} \\ &= (1 - q^{-2\ell_{m_i}})^{q^{2\ell_{m_i}} \cdot \frac{m_i}{\ell_{m_i} q^{2\ell_{m_i}}}}. \end{aligned}$$

Since $\lim_{i \rightarrow \infty} \frac{\log_q m_i}{\ell_{m_i}} = 0$ (which implies that $\lim_{i \rightarrow \infty} \ell_{m_i} = \infty$), we see that

$$\lim_{i \rightarrow \infty} \frac{m_i}{\ell_{m_i} q^{2\ell_{m_i}}} = \lim_{i \rightarrow \infty} q^{-\ell_{m_i} \left(2 - \frac{\log_q m_i}{\ell_{m_i}} + \frac{\log_q \ell_{m_i}}{\ell_{m_i}} \right)} = 0.$$

Note that $(1 - q^{-2\ell_{m_i}})^{q^{2\ell_{m_i}}} > 1/4$. We get that

$$\lim_{i \rightarrow \infty} \Pr(\dim C_{a,a'}^{(i)} = m_i - 1) \geq \lim_{i \rightarrow \infty} (1/4)^{\frac{m_i}{\ell_{m_i} q^{2\ell_{m_i}}}} = 1. \quad \square$$

From Theorem 3.3 and Theorem 3.4, we obtain the following at once.

Theorem 3.5. *Let δ be a positive real number such that $\delta < \frac{2}{3}h_q^{-1}(\frac{1}{2})$. Then there is a sequence of quasi-cyclic codes C_i of index $1\frac{1}{2}$ over F for $i = 1, 2, \dots$ such that the co-index of C_i goes to infinity and the following hold.*

- (i) $\lim_{i \rightarrow \infty} R(C_i) = \frac{1}{3}$;
- (ii) $\Delta(C_i) > \delta$ for all $i = 1, 2, \dots$.

For example, if take $q = 3$, then $0.106 < \frac{2}{3}h_q^{-1}(\frac{1}{2}) < 0.107$; so we can take $\delta = 0.106$, and get a sequence C_1, C_2, \dots of quasi-cyclic ternary codes of index $1\frac{1}{2}$ such that the length of C_i goes to infinity, $R(C_i) \rightarrow 1/3$, and $\Delta(C_i) > 0.106$ for all $i = 1, 2, \dots$.

Acknowledgements

The research of the authors is supported by NSFC with grant numbers 11271005.

References

- [1] L. M. J. Bazzi, S. K. Mitter, “Some randomized code constructions from group actions”, *IEEE Trans. Inform. Theory*, vol.52, pp.3210-3219, 2006.
- [2] C.L. Chen, W.W. Peterson, E.J. Weldon, “Some results on quasi-cyclic codes”, *Information and Control*, vol.15, pp407-423, 1969.
- [3] V. Chepyzhov, “New lower bounds for minimum distance of linear quasi-cyclic and almost linear quasi-cyclic codes”, *Problemy Peredachi Inform.*, vol.28, pp33-44, 1992.

- [4] B. K. Dey, B. S. Rajan “Codes Closed Under Arbitrary Abelian Group of Permutations”, *Siam J. Discrete Math.*, vol.18, pp1-18, 2004.
- [5] Yun Fan, Liren Lin, “Thresholds of random quasi-abelian codes”, *IEEE Trans. Inform. Theory*, vol.61, no.1, pp.82-90, 2015.
- [6] Yun Fan, Yuan Yuan, “On self-dual permutation codes”, *Acta Mathematica Scientia*, vol.28B, pp633-638, 2008.
- [7] W. C. Huffman, V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, 2003.
- [8] T. Kasami, “A Gilbert-Varshamov bound for quasi-cyclic codes of rate $1/2$ ”, *IEEE Trans. Inform. Theory*, vol.20, p679, 1974.
- [9] San Ling, P. Solé, “Good self-dual quasi-cyclic codes exist”, *IEEE Trans. Inform. Theory*, vol.49, pp.1052-1053, 2003.
- [10] C. Martínez-Pérez, W. Willems, Is the Class of Cyclic Codes Asymptotically Good? *IEEE Trans. Inform. Theory*, vol.52, pp.696-700, 2006.
- [11] C. Martínez-Pérez, W. Willems, “Self-dual double-even 2-quasi-cyclic transitive codes are asymptotically good”, *IEEE Trans. Inform. Theory*, vol.53, pp.4302-4308, 2007.
- [12] B.R. McDonald, *Finite Rings with Identity*, New York: Marcel Dekker, 1974.
- [13] M. Mitzenmacher, E. Upfal, *Probability and Computing: Randomized Algorithm and Probabilistic Analysis*, Cambridge Univ. Press, Cambridge, 2005.
- [14] R. R. Varshamov, “Estimate of the number of signals in error-correcting codes” (in Russian), *Dokl. Acad. Nauk*, vol.117, pp.739-741, 1957.
- [15] S. K. Wasan, “Quasi Abelian codes”, *Publ. Inst. Math. (Beograd) N.S.*, vol.21, pp201-206, 1977.